Bulldog Home GRIPs Engagement

November 2023

Agenda

1. Introductions
2. Executive Summary
3. NIST Cybersecurity Framework Maturity Assessment
4. Risks & Recommendations
5. Roadmap
6. Recap

Executive Summary

What did we do? What approach did we use?

The team was requested to conduct a consolidated NIST maturity model on Bulldog Home's environment to understand the current security state and identify opportunities to improve. The maturity assessment included four meetings with four security domains that span across the 5 NIST functions whom were interviewed to determine a maturity level, associated gaps, recommendations to address and remediate gaps, and a roadmap with prioritized action items to reach the target end state.

Domains	Key Gaps
What security domains were assessed?	What current gaps are associated with each security domain?
User and Network Access	Access Management & User Privileges
Security Operations	Network & Security Monitoring
Governance, Risk and Compliance & Vulnerability Management	Asset & Vulnerability Management
Business Continuity and Disaster Recovery	Documented Response and Recovery Planning

NIST Framework Elements

NIST Framework elements	Identify	Protect	Detect	Respond	Recover
Category data level	1-5 CMMI	1-5 CMMI	1-5 CMMI	1-5 CMMI	1-5 CMMI
Function Description	**What matters most to our business, and what are our biggest threats?**	**What measures have we taken to confirm that key elements of our business are safe?**	**How alert are we to threatening events or potential disruptions?**	**How quickly and effectively can we react when bad things happen?**	**Once we've experienced an attack or disruption, how quickly will we be able to resume normal operations?**
Subcategories	▪ Asset Management ▪ Business Environment ▪ ***Governance** ▪ ***Risk Assessment** ▪ Risk Management Strategy	▪ ***Access Control** ▪ ***Awareness and Training** ▪ Data Security ▪ Information Protection Processes and Procedures ▪ Maintenance ▪ Protective Technology	▪ ***Anomalies and Events** ▪ Security Continuous Monitoring ▪ ***Detection Processes**	▪ ***Response Planning** ▪ Communications ▪ ***Analysis** ▪ Mitigation ▪ ***Improvements**	▪ ***Recovery Planning** ▪ Improvements ▪ **Communications**

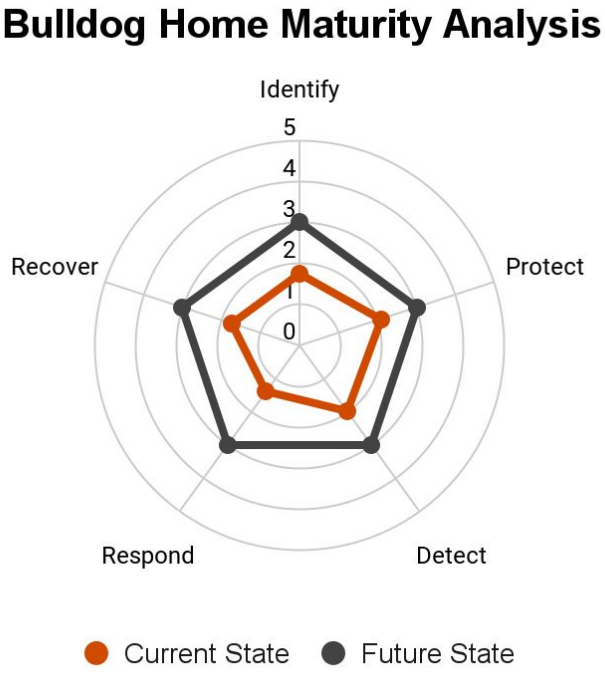
*Subcategories assessed for this engagement

CMMI maturity-level definitions

5. Optimizing:	Process improvement incorporated to make process more effective as SOP
4. Managed:	Processes consistently managed and measured for performance consistency
3. Defined:	Processes consistently managed/performed
2. Repeatable:	Processes inconsistently managed/performed
1. Ad Hoc:	Processes lack sustainable, consistent management

Current State Maturity Rating

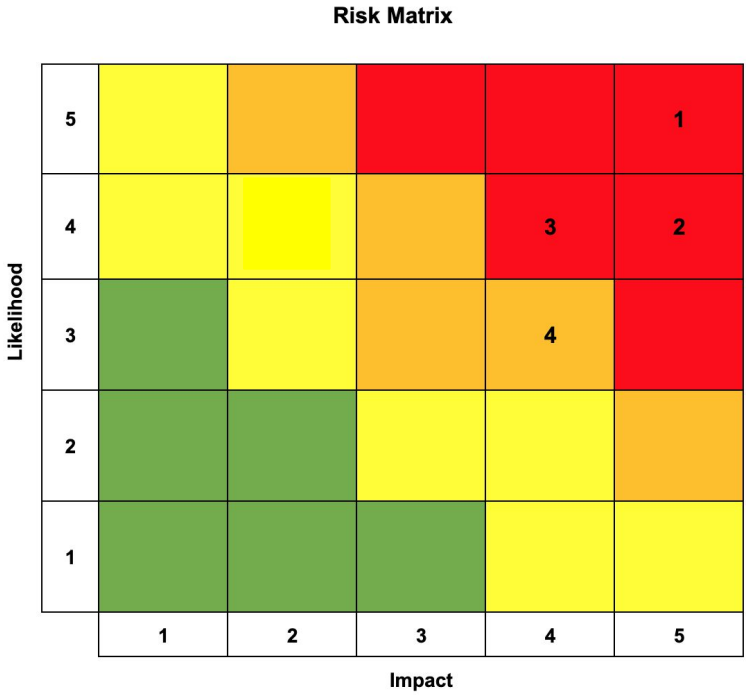
Functions	Rating	Observations
Identify	1.78	Bulldog Home does not have a formal governance framework for cybersecurity, and there is a lack of regular risk assessments and vulnerability scans.
Protect	2.09	BH has some formal processes in place for access control and password management, but there is room for improvement in terms of access control policies, user access privilege reviews, and password management.
Detect	2.00	BH handles security events manually, often without a clear understanding of the root cause or potential impact.
Respond	1.38	BH's incident response processes are ad hoc and unstructured, leading to delayed responses and potential data loss.
Recover	1.75	BH does not have any formal business continuity and disaster recovery plans, and recovery time objectives (RTOs) and recovery point objectives (RPOs) are determined by the organizations experience.



Capabilities Maturity Workbook

Risks

	Risk	Associated Security Domain
1	Event Management	Security Operations
2	Disrupted Business Operations	Business Continuity and Disaster Recovery
3	Vulnerability Management	Governance, Risk and Compliance & Vulnerability Management
4	Access Management and User Privileges	User and Network Access



[Capabilities Maturity Workbook]

Security Operations

Key Risks	Recommendations	Security Benefits
Event Management • SOC analysts manually check multiple dashboards to identify events and there are not alert thresholds in place • No event log aggregation which makes event analysis inefficient	**SIEM (Security Information and Event Management) Tool** • Aggregation and analysis of data across the BH environment • Identifies anomalies and generates threat alerts	**Improved Anomalies and Events Maturity** • Event data is aggregated from multiple sources to facilitate efficient event analysis **Improved Analysis Maturity** • Alerts produced by SIEM tool will decrease threat response time
• No threat prioritization so security alerts are responded to as they appear	**Develop Threat Prioritization Process** • Documented process for prioritizing event response	**Improved Risk Assessment Maturity** • Facilitates resource allocation to the threats that are of the highest risk
Security Operations Center Manpower • SOC is a team of two employees that also support other areas within BH's Security Department • Responsible for monitoring and responding to security events within BH Environment • Substantial responsibilities places on the SOC team members can lead to overlooked vulnerabilities and inefficient incident responses	**Hire Additional SOC Analyst** • Additional manpower to assess and respond to threats • Opportunity to define roles and responsibilities within SOC team	**Additional SOC Resources** • Decreased probability of fatigue-induced errors • Opportunity for definition of roles within SOC team to spread responsibilities across team to improve detection process

Business Continuity and Disaster Recovery

Key Risks	Recommendations	Security Benefits
Business Continuity Plan & Disaster Recovery Plan • Lack of formally documented BCP or DRP • Undefined recovery processes • No designated party responsible for responding to incidents	**Business Continuity Plan** • Comprehensive document outlining how to ensure the continuation of business operations • Regularly updated and tested • Clarifies roles and responsibilities **Disaster Recovery Plan** • Focused on restoring critical functions • Outlines actions needed to be taken in order to limit damages and recovery efficiently and effectively	**Improved Response and Recovery Maturity** • Better preparation and response capabilities to various disaster scenarios • Reduced downtime and operational impacts during the event of an incident • Increased effectiveness and efficiency of recovery from an incident

Communication Processes
• Communication processes not fully integrated throughout all business units
  • Exclusive for company executives
 	
Incident Impact Analysis
• No defined analysis or processes
  • Incidents and Resolutions
	Business Impact Strategy
	• Develop clear communication processes
	  • Improve communication throughout all levels
	
	• Develop incident analysis process
	  • Documents incidents and resolutions
	  • Improved management and categorization of events
		Improved Response Analysis Maturity
		• Improved cohesiveness resulting in enhanced fluidity of business operations
		
		• Lessons learned can be leveraged into an opportunity to improve response plans
		• Enhanced response and resolution protocols
		  Quicker return to normal business operations

Governance, Risk and Compliance & Vulnerability

Key Risks	Recommendations	Security Benefits

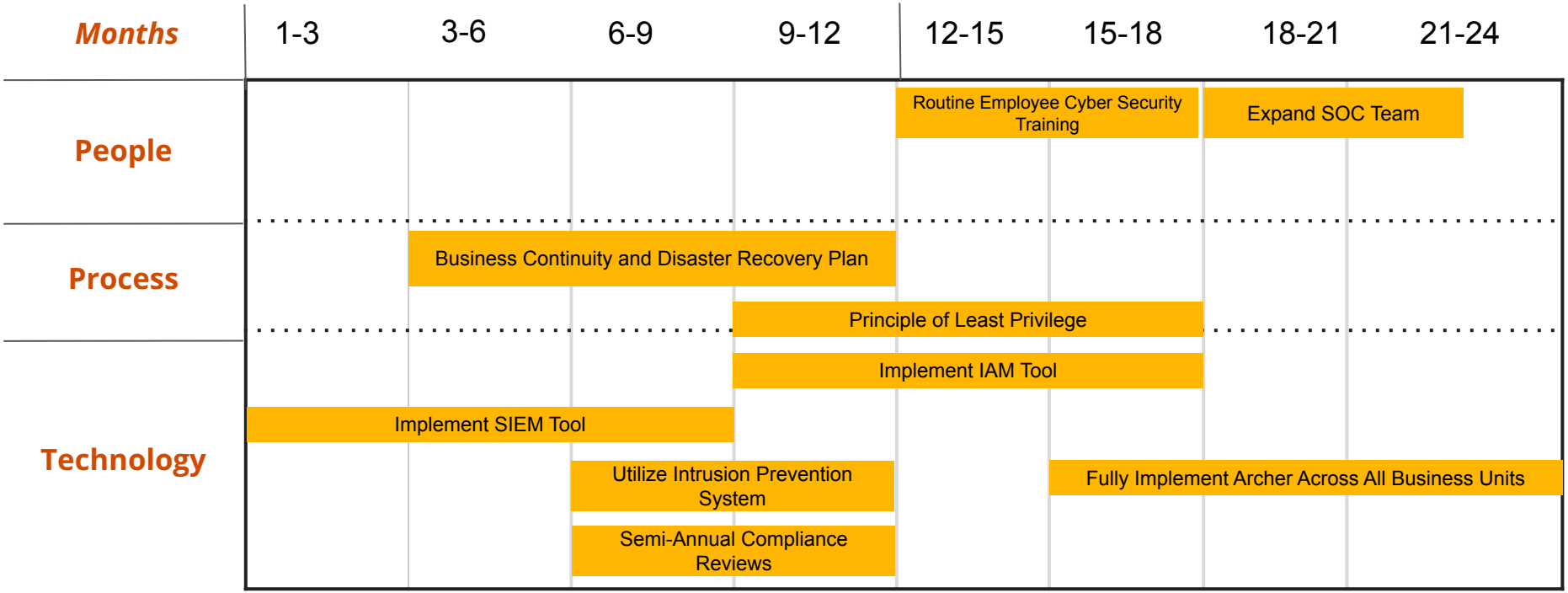
Compliance Monitoring and Maintenance
• Improper documentation of compliance processes
• Lack of a centralized approach when engaging with third parties
• Failure to conduct due diligence and stay updated with external stakeholders
 	
Asset Management
• Lack of centralized enterprise-wide asset inventory
	Archer (Third Party Management Tool)
	• Expert Third Party Consultation
	• Ensures compliance requirements are met
	  ○ Frequent checks with legal and regulatory changes
	• Improves and maintains third-party relationships
	
	Centralized Asset Repository
	• Enhanced management of company assets and allocated resources
		Improved Governance Maturity
		• Enhanced management of external partners
		  • Improved selection of vendors
		• Builds trust and transparency
		• Strengthened third party compliance and and adherence to industry best standards
		
		• Solidify and maintain awareness of state of assets
		  • Vulnerabilities associated

Cyber Security Awareness
• Majority of training appears to be optional
  • Exclusive for leadership
• Awareness of security related roles and responsibilities are held at a basic level of understanding
	Employee Cybersecurity Training
	• Essential and regularly updated training
	• Educate privileged users on why and how to utilize their responsibilities correctly
	• Leadership to lower-level employee involvement
	  • Security best practices
	  • Bolster overall security
		Improved Awareness and Training Maturity
		• Knowledge of security best practices throughout the entire company will be held at a more cohesive understanding
		• Strengthens and improves security from the inside out
		• Improves relationships with stakeholders showing BH's high-level security mindset

User and Network Access

Key Risks	Recommendations	Security Benefits
Access Controls • New user access rights are cloned off an existing user rather than user specific • Most user have administrative access to systems	**Principle of Least Privilege** • Limit user access to the systems and data that is necessary to complete individual's responsibilities	**Improved Access Control Maturity** • Incorporating principle of least privilege limits attack surface area by limiting access points
• Currently no user privilege tracking • Approval requests are documented by storing emails • Access removal for terminated employees takes a week due to insufficient staffing	**Identity Access Management (IAM) Tool** • Provide centralized access control management of user access rights • Facilitate timely user access granting and revoking	• Improved access permissions management resulting in reduced data and system access
Network and Security Monitoring • Intrusion Detection System (IDS) is in place • IDS system is currently only utilized to monitor network traffic • A cumulative weekly report of suspicious traffic is sent to security team	**Intrusion Prevention System (IPS)** • Utilize full IPS capabilities to block malicious traffic from accessing the environment • Connects to recommended SIEM tool to provided real-time incident alerts to Security Operations Center analysts	**Improved Detection Process Maturity** • Proactively prevent malicious traffic from accessing • Event detection alerts will be efficiently communicated to SOC analysts

Roadmap



[Budget]

Recap

Engagement Summary	**Our six-week engagement with Bulldog Home revealed vulnerabilities in access controls, security awareness, and risk management. Despite the identified vulnerabilities, the organization demonstrates a strong commitment to aligning with cybersecurity standards, signaling a proactive stance in addressing their cybersecurity challenges.**
Recommendations	**Implementing Archer across all business units, establishing a vulnerability management plan, engaging in cybersecurity training, deploying an SIEM tool, expanding the SOC team, and documenting plans are actions to fortify BH's security posture to ensure a resilient and proactive defense against cybersecurity threats.**
Value Added	**Our two-year plan includes plans to efficiently automate processes through various systems and tools, minimize any potential risks, and secure Bulldog Home's valuable assets.**

Thank you!

Questions?

Budget

EXPENSE	AMOUNT	TYPE	TOTAL	NOTES
Asset Management Software	$500,000	per year	$500,000	Software for managing physical and IT assets
SIEM Tool	$1,000,000	one time	$1,000,000	SIEM tool will help with real time analysis of security alerts and better prioritize threats.
Threat and Risk Prioritization	$500,000	per year	$500,000	Tool for prioritizing threat alerts - utilize Archer to fullest extent
Hire PR Executive	$250,000	1 employees/per year	$250,000	Employees to help support our new implementation (SOC analyst, Incident Response, Cyber IT Specialist)
Hire SOC Analyst	$100,000	1 employee/per year	$100,000	Provide assistance in the Security Operations Center
Cyber Security Employee Training	$300,000	one time	$300,000	Creating a structured and dynamic training program
Post Implementation Testing	$500,000	one time	$500,000	Testing to ensure there are no gaps once recommendations have been implemented
Assistance for Business Impact Analysis/Disaster Recovery Plans	$300,000	one time	$300,000	Third party help for creating proper plans and strategies
IAM Tool	$1,000,000	one time	$1,000,000	AIM tool will help strengthen access controls and implement principle of least privilege
		Total:	**$4,750,000**	

BullDog Home Maturity Analysis